Bluezone – Close contact detector

1. Introduction

The situation of COVID-19 pandemic continues complicated developments. As of August 3, 2020, there are about 17.9 million cases of SARS-CoV-2 around the world. Up to the afternoon of August 3, 2020, Viet Nam has confirmed 642 cases of SARS-CoV-2, of which there are 373 recoveries and 6 deaths.

During the teleconference between the country's National Steering Committee for COVID-19 Prevention and Control and its 63 provinces and cities April 17, 2020, Deputy Prime Minister Vu Duc Dam – who heads the Committee – stressed: The pandemic is sure to last long. Despite it might be settled down at times and in different locations, the pandemic ends only when medicines or vaccines become available. This is critical because we cannot just shut our doors while needing to find ways to accomplish the 'double goals'. That means we must manage to control the pandemic, coexist safely with it and embrace positive changes in the society.

Whereas, Prime Minister of Viet Nam, Nguyen Xuan Phuc, has asked for continued implementation of mandatory quarantine for all passengers entering the country. He also requests early identification and treatment for COVID-19 cases, especially the applying of information technology in tracing infections, thereby gradually loosening containment measures to help the life return to normal.

2. Contact tracing solutions

According to statistics from different epidemic regions in the world, the reproduction rate of SARS-CoV-2 ranges from 2.5 to 4, meaning the virus can be transmitted from 1 person to 2 to 4 others. The transmission process can take place since the symptoms are still mild, with some patients having no symptoms (signs of illness) at all.

To reduce SARS-CoV-2 spread in the context of social distancing measures being loosened, there is a need for technology solutions to be put in place to help control people's contacts with the community. Such solutions shall enable the fastest and most complete identification of those in risk when a case of infection is confirmed.

Smartphone is a popular item in people's life. Therefore, developing applications for smartphones to help halt the spread of COVID-19 is an effective approach. Through the smartphones, human-to-human contacts can be determined by using solutions such as GPS, Cell phone position (BTS), Bluetooth low energy.

Global Positioning System (GPS) helps determine location based on signals by artificial satellites. Its accuracy is greatly affected by the weather and surroundings, with location errors reaching tens of meters for indoor places or in negative weather conditions.

Cell phone positioning system determines locations by utilizing the signals of base transceiver stations (BTS). Its accuracy depends on the density of such stations, with errors reaching hundreds of meters in some cases.

BLE (Bluetooth low energy) is a power saving and short-range technology that operates stably in a distance up to 10 meters and helps to transmit small loads of data. The technology is suitable for intermittent control applications and is now integrated in almost all smartphone products.

BLE has many advantages: high accuracy (in meter-level), possible to identify close proximity within a 2-meter radius; ensuring privacy (does not utilize the precise location of users, works by recording close contacts and time, duration of such contacts); possible to be used daily due to its low energy consumption.

BLE is also the solution that Europe, USA and Singapore have started to research and apply in the combat against COVID-19, especially for the purpose of helping life return to normal after the peak of the epidemic. In addition, two technology companies that own 99% of smartphone users in the world, Apple and Google, have worked together to develop a technology using BLE to join hands with other companies to fight COVID-19.

BLE technology helps identify exactly who needs to be put in quarantine. Instead of quarantining thousands to tens of thousands of people when a case of infection is confirmed, with the help of BLE, we now can pick out those who had real close contacts. As a result, the outbreak can be ended in an accurate and effective way, getting life back to normal.

3. Overview of Bluezone system

Bluezone is an app that uses Bluetooth low energy technology to serve the prevention and control of COVID-19, thereby protecting the community against the pandemic.

3.1 Description of the system

Smartphones with Bluezone installed can communicate with each other within a distance of 2 meters, recording close contacts as well as the time and duration of such contacts. When a new case of SARS-CoV-2 is confirmed, health authorities enter this F0 data into the system. The system then sends such F0 data to other smartphones with Bluezone. The history of exposure to F0 in the previous 14 days will be analyzed, compared and if matched, Bluezone will alert users at risk of infection and instruct them to contact health authorities to get help.

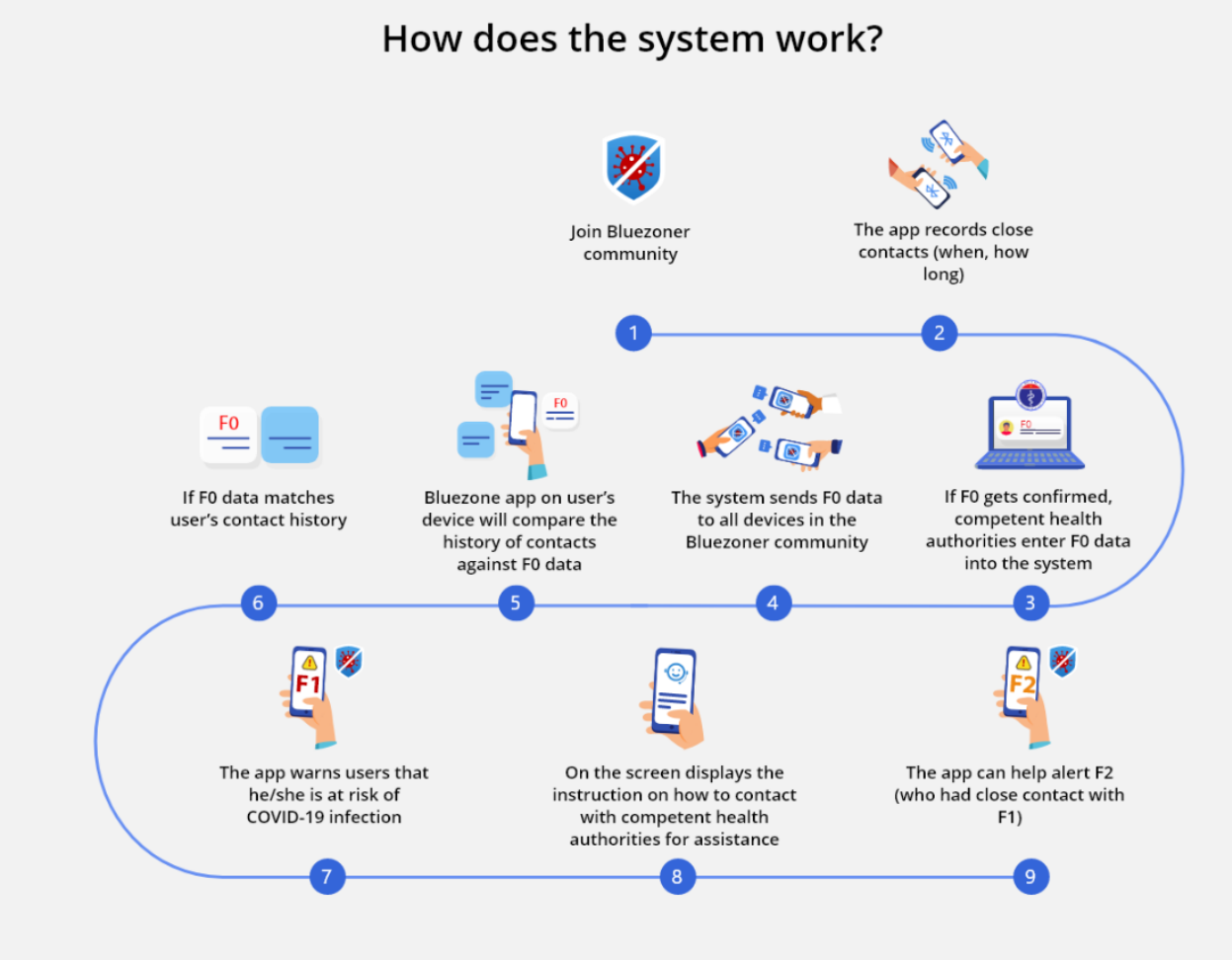


Figure 1: Operation model of Bluezone

3.2 Bluezone principles

The birth of Bluezone comes from the philosophy called 'Protect yourself, protect the community': The app shall alert you if you had close contact with people who have SARS-CoV-2. By joining the community, you have got connected to protect the community, protect the world.

The operation of Bluezone is based on the following principles:

Data secured: The data of your contact history is stored on your device only and will not get transmitted to the system. When installing Bluezone, you are advised to provide your contact details (name, phone number, address) in order to get direct support in case you got infected with or exposed to COVID-19.

No location data collection: The app does not collect data on your location

Anonymity: People joining the community will remain anonymous to others. Only competent health authorities are able know the identities of infected people as well as of those who are suspected of infection due to close contact with COVID-19 cases.

Transparency: The project is open source under GPL 3.0 license. Users of countries around the world are free to learn about system activities at the source code level, and to use, research, modify and share it.

4. Bluetooth contact tracing algorithm

4.1 Description of Bluezone technology

Each Bluezone smartphone takes on 2 roles, ***Peripheral*** (broadcasting device) and ***Central*** (receiving device).

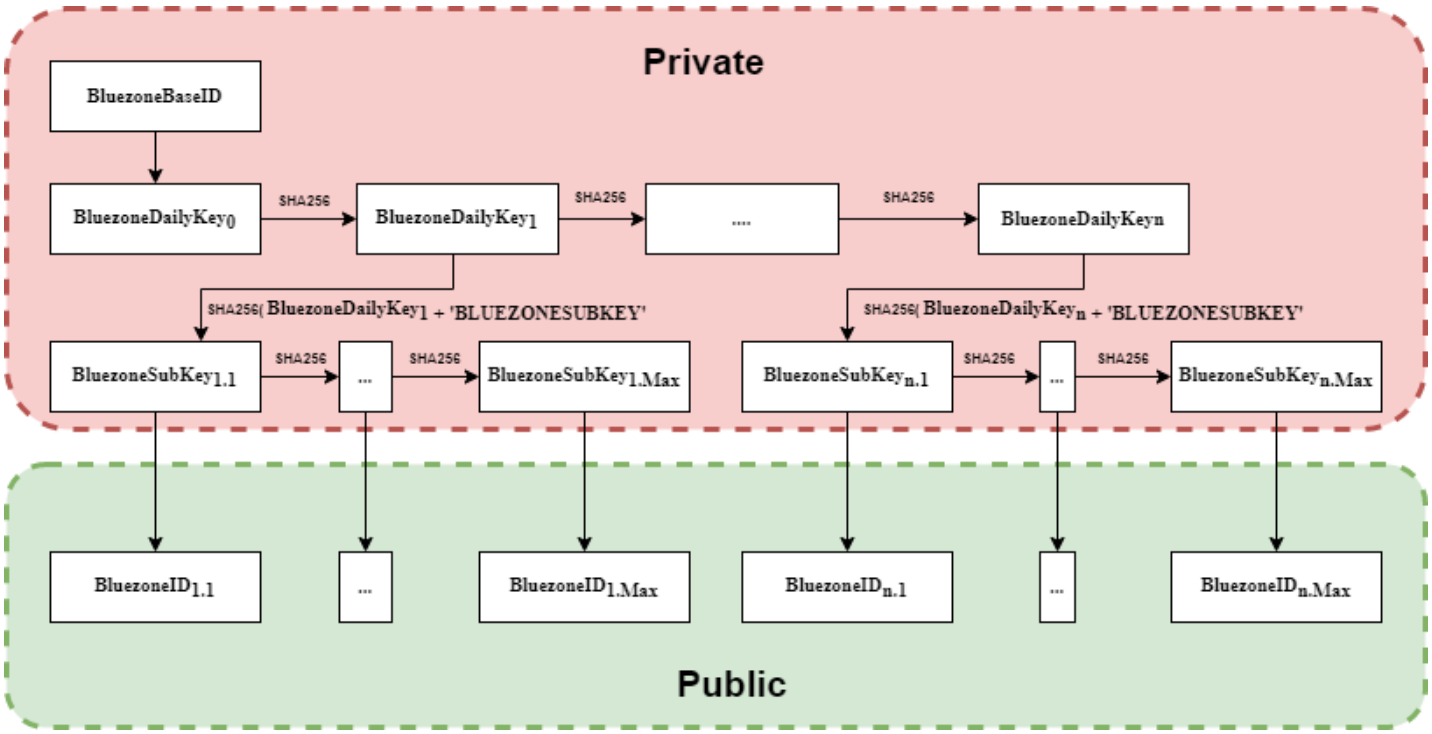
The broadcasting device will generate a random Bluezone Id (BLID), which will change after a period of time (in Viet Nam, BLID changes every 15 minutes). Each BLID has a length of 12 bytes (to be explained below). The BLID of this broadcasting device will be recorded and stored by other receiving devices for the sake of later close contact identification in case F0 is confirmed.

The BLID generation algorithm changes over time as follows:

4.1.1 Interpretation

- **BluezoneBaseID**: A random key for each user with the length of 256 bits, not shared with anyone.
- **D_0:** The day that Bluezone is installed.
- **$BluezoneDailyKey_n$:** F0 A key changes daily, generated from BluezoneBaseID. This key will be used in case of F0 detection.
- **Max**: Total IDs generated in 01 day; the number is 96 by default - equivalent to changing ID every 15 minutes
- **BluezoneID (BLID)** is generated daily according to timelines so that the total number of BluezoneID in a day reaches **Max**.
- **D_k:** The day starting epidemiological investigation with 1 F0 detected.
- **T_e:** The time F0 is confirmed by the health staff and F0 information is pushed into the system to search for F1.

4.1.2 Details of BLID generation algorithm



Step 0: Generate BluezoneBaseID when a user installs Bluezone.

Step 1: **BluezoneDailyKey is generated daily** according to the following formula:

$$\textbf{BluezoneDailyKey}_n = \text{SHA256}(\textbf{BluezoneDailyKey}_{n-1})$$

Step 2: Depending on the number of IDs changing daily (configured from server), the sub-Key number is generated correspondingly (for example, changing ID every 15 minutes will generate 96 sub-Keys). The sub-Key generation formula is as follows:

$$\textbf{BluezoneSubKey}_{n.1} = \textbf{SHA256(BluezoneDailyKey}_n\textbf{+ 'BLUEZONESUBKEY')}$$

$$\textbf{BluezoneSubKey}_{n.i} = \textbf{SHA256 (BluezoneSubKey}_{n.i-1}\textbf{)}$$

Step 3: Generate BLID to broadcast, receive and store as a byte array with the length of 12 bytes according to the principle: Get bytes at positions 0, 4, 8, 12, 16, 18, 20, 22, 24 , 26, 28, 30 in **BluezoneSubKey**'s 32-byte array as values for 12 bytes of **BLID.**

4.2 Contact tracing

When F0 is detected, the Health Authority updates (**BluezoneDailyKey$_k$, D_k, Max, T_e**) to the system. In which, D_k is the day starting epidemiological investigation (for example, 14 days from the detection day of F0), **BluezoneDailyKey$_k$** is the corresponding key of F0 at the time of D_k, T_e

is the time of confirming F0 information. Contact histories with F0 after this point will be invalid as F0 will be exchanged for another BluezoneBaseID from the time of T_e. **Max** is the number of BluezoneIDs generated in 1 day.

The system will then broadcast the digital set (**BluezoneDailyKey$_k$, D$_k$, Max, T_e**) to all Bluezoners. Bluezoners will rely on (**BluezoneDailyKey$_k$, D$_k$, Max, T_e**) to generate DailyKey => SubKey => BluezoneID with the Max number of BluezoneID for 1 day according to the algorithm in Section 4.1.2.

Each BLID of F0 will only be valid for a specified period of the day, this time is determined as follows:

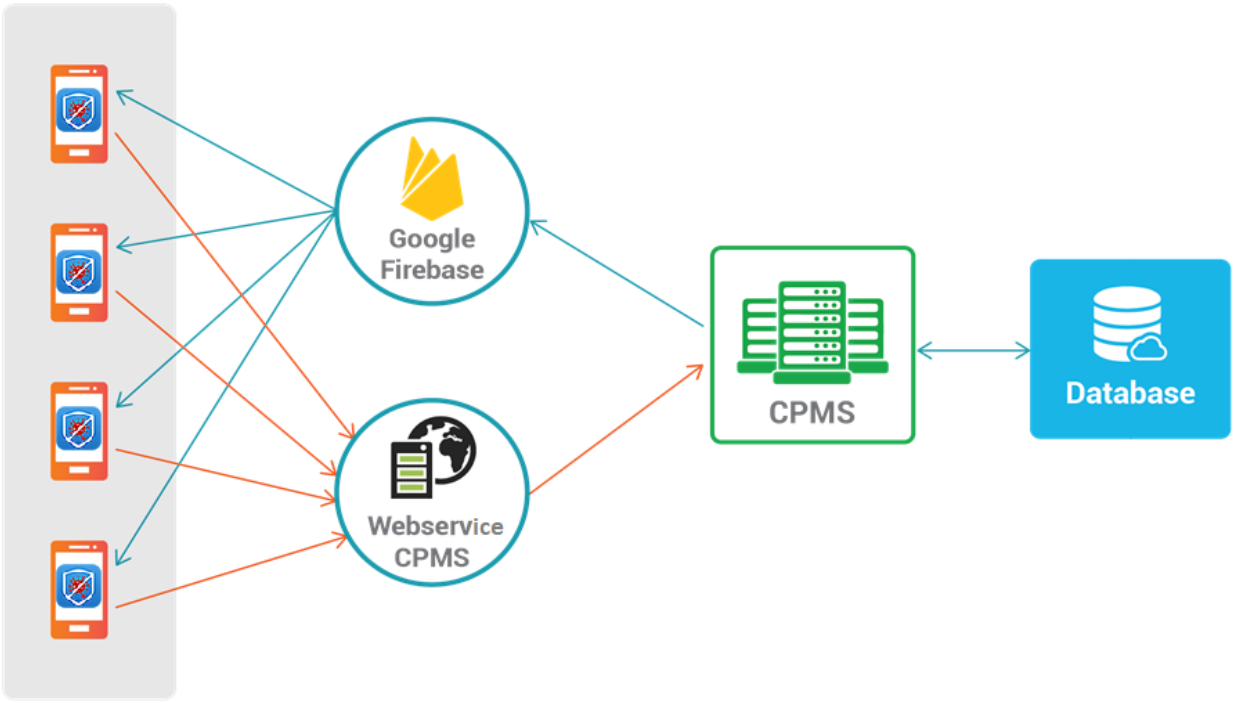
- Interval between two consecutive times generating **BLID** in the day is: $\Delta t = \frac{24*3600*1000}{Max-1}$
- $BluezoneID_i$ (the i times of generation in the day) is only valid to record contacts in the time range from $(i - 1)* \Delta t$ to $i *\Delta t$
- If the contact history of a user records $BluezoneID_i$ of F0, and the contact time recorded is t, the user will be confirmed to have contact with F0 if and only if: $(i - 1)*\Delta t \leq t < i*\Delta t$ và $t < T_e$

4.3 Overcome the "weaknesses" of other existing BLE contact tracing solutions

We recognize that BLE solutions of other groups/organizations in the world that have been implemented in reality are not complete due to insufficient contact records. Specifically, if iOS users want to keep track of their contacts, they need to let the BLE application run in foreground to record other devices. To solve this issue, the teams recommend that users always turn on the app in the foreground, which means users must run the app and keep the screen light all the times. This is an unrealistic approach that few people can cope with. First, it wastes battery when the screen has to be constantly on. Second, users can do nothing else with their smartphone when the application is always in foreground.

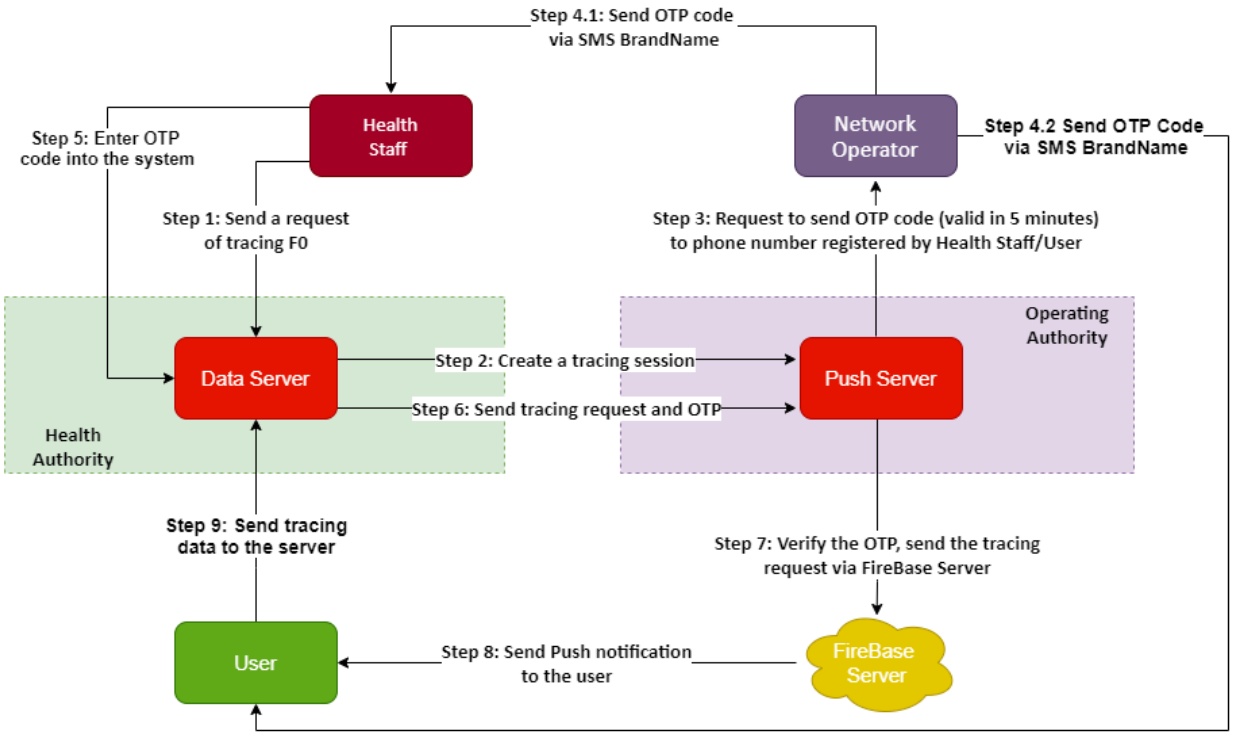
First of all, we have resolved this problem to make the iOS Bluezone version able to record contacts (if any) with other Android devices even when in background mode. The results are positive. Next, Android Bluezone is also designed to recognize iOS Bluezone devices while running in the background. Finally, foreground-running iOS Bluezone can recognize other background-running iOS devices (Refer to the table of contact cases in section 7.1). By using the bridging principles like this, we can trace almost all user contacts without requiring the iOS app to be always turned on in foreground mode.

5. Bluezone Backend system



Bluezone Backend scenarios: (CPMS - COVID-19 Proximity Monitoring System)

Upon official confirmation of an F0, competent health staff will access the CPMS system to update this F0's details by using F0 information entering function of the Backend CPMS system.



The process of updating F0 information to the system consists of 9 steps as follows:

Step 1: The health staff creates a request of entering F0 information.

Step 2: Data Server (administered by the Health Authority) sends a request of creating F0 data updating session. Between Data Server and Push Server survives a secure data transmission with encryption and anti-denial authentication.

Step 3: Push Server (administered by the Operating Authority) creates a request for authentication by one of the following 2 ways:

- Option 1: an OTP is generated for the F0 to actively send his/her information to Data Server.

- Option 2: an OTP is generated for a competent person to allow the obtaining of the F0's information (in some cases, the F0 might have got too ill to open his/her own device to submit the data).

Step 4: The network operator sends OTP code via SMS BrandName to the device of the F0 or of the competent person.

Step 5: The competent person confirms by entering the OTP, or provides the OTP for the health staff to do the confirmation.

Step 6: Data Server sends Push Server the request of entering F0 information and OTP code.

Step 7: Push Server sends Push Notification request to FireBase Server – the server that manages the notifications.

Step 8: FireBase Server sends notifications to the user's phone.

Step 9: The user's phone sends F0 information to the Health Authority.

Upon receiving F0 information, CPMS system will broadcast F0 information (as described in Section 4.2) to all clients.

The client receives CPMS notification and then processes the information. In case no contact with that F0 is found, the software does not need to do anything further. Otherwise, the software will display a notice and ask the user to push his/her contact history to servers according to the data security mode configured (specifically mentioned below). Such data will then be cleaned and compared to identify F1s and add them to the list to be processed.

Data security policy:

1. Option to push information to servers of F1s: The system allows configuring F1s' confirmation regarding information provision. This property will be configured based on each country's data security policy.
2. There are 2 modes for providing data of contact history to servers:
    a. Mode 1: contact history with F0.
    b. Mode 2: the entire contact history of F1.

6. Security and privacy assurance

6.1 Privacy assurance

All contact history data is stored only on the user's smartphone, not transferred to a centralized storage system. The app also does not collect user location data. People joining the community will remain anonymous to others. Only competent health authorities can know those who are infected and or are suspected of infection through close contact with COVID-19 cases.

6.2 Other security issues

Risk of unfair-play. An unhandled concern raised by contact tracing developing team is that: a bad actor might record Bluezone IDs of all patients visiting a health facility, for example setting up a BLE receiver here, then locates a Bluetooth broadcasting device in a public place or at an opponent's workplace. This device will broadcast Bluezone signals that fakes the Bluezone IDs collected earlier. If unfortunately, one of the Bluezone IDs from the health facility is confirmed to be F0, all those who unknowingly receive this Bluezone ID will be warned as F1, causing them trouble and worry.

The solution we offer: Supposing a Bluezoner gets an alert via broadcasting saying that he/she had contact with a F0, this Bluezoner will be provided with an option to verify such F0 by committing his/her contact history with that F0 to the system for comparison with F0 contact history updated by health authorities. If it does not match, that Bluezoner is not a F1.

Risk of fake declaration. If person A for some reason deliberately declares himself to be infected with COVID-19 and sends fake data to the center, such fake data can cause spam and generate fake alerts for people who had contact with A.

To solve this problem, F0 data will only be updated by health authorities, no one can commit their own data to the center if health authorities have not confirmed through a standardized test result.

7. Compare to other solutions

7.1 Effectively recording close contacts

The recording of ***BLID*** information via BLE broadcast packet only without connection makes the contact recording faster and more energy-efficient, avoiding missed cases. While other existing

solutions in the world must fully implement the connection to be able to record contacts, leading to battery consumption and easily missed cases.

The story of tracing using Bluetooth BLE is not only about algorithms to ensure privacy, the biggest problem is to ensure efficiency in reality. As mentioned above, most current solutions of other countries are limited to recognizing devices running Android, and for iOS devices, the screen must be on and the app must run continuously, which does not guarantee effectiveness in implementation.

In about 3 weeks of running on schedule, the teams of Viet Nam have made efforts to solve the above-mentioned weaknesses, together with the determination of MIC, and the regular urge on and encouragement to teams directly by the Minister. The results are encouraging when most teams of Viet Nam found out solutions to the above complex problem. This also confirms the competence of Vietnamese ICT engineers.

We implemented the test cases as below to record contacts in real situations. We used one phone to record the contact with the other two phones, with the aim of ensuring the recording is done properly and sufficiently. Most of the test cases have been passed, showing the ability of recording in reality is very good. Only 3/24 case do not record contacts, specifically when iOS devices are in the background, they do not recognize other iOS devices. This has also been analyzed above (see Section 4.3), we will deal with other cross-contact cases between iOS and Android, as well as between background iOS and other foreground iOS (cases 7, 8, 9, cases 16, 17, 18, and cases 22, 23, 24).

NO.	Device	Case	Result
1	1 Android scans 2 Androids	(1 running Bluezone in the foreground) scans (2 running the app)	Proper and sufficient recording
2		(1 running Bluezone in the foreground) scans (2 with screen off)	Proper and sufficient recording
3		(1 running Bluezone in the foreground) scans (2 with screen on and in standby mode)	Proper and sufficient recording
4		(1 with screen off) scans (2 with screen off)	Proper and sufficient recording
5		(1 with screen off) scans (2 with screen off, app running in the background)	Proper and sufficient recording

6		(1 with screen on, app running in the background) scans (2 with screen off)	Proper and sufficient recording
7	1 iOS scans 2 iOSs	(1 running Bluezone) scans (2 running the app)	Proper and sufficient recording
8		(1 running Bluezone) scans (2 with screen off)	Proper and sufficient recording
9		(1 running Bluezone) scans (2 with screen on, app running in the background)	Proper and sufficient recording
10		(1 with screen off) scans (2 with screen off)	No recording, but will be solved through cases in contact with other Android, as well as by cases recorded by other iOSs in the foreground.
11		(1 with screen off) scans (2 with screen on, app running in the background)	No recording, but will be solved through cases in contact with other Android, as well as by cases recorded by other iOSs in the foreground.
12		(1 with screen on, app running in the background) scans (2 with screen off)	No recording, but will be solved through cases in contact with other Android, as well as by cases recorded by other iOSs in the foreground.
13	1 iOS scans 2 Androids	(1 running Bluezone) scans (2 running the app)	Proper and sufficient recording
14		(1 running Bluezone) scans (2 with screen off)	Proper and sufficient recording
15		(1 running Bluezone) scans (2 with screen on, app running in the background)	Proper and sufficient recording
16		(1 with screen off) scans (2 with screen off)	Proper and sufficient recording

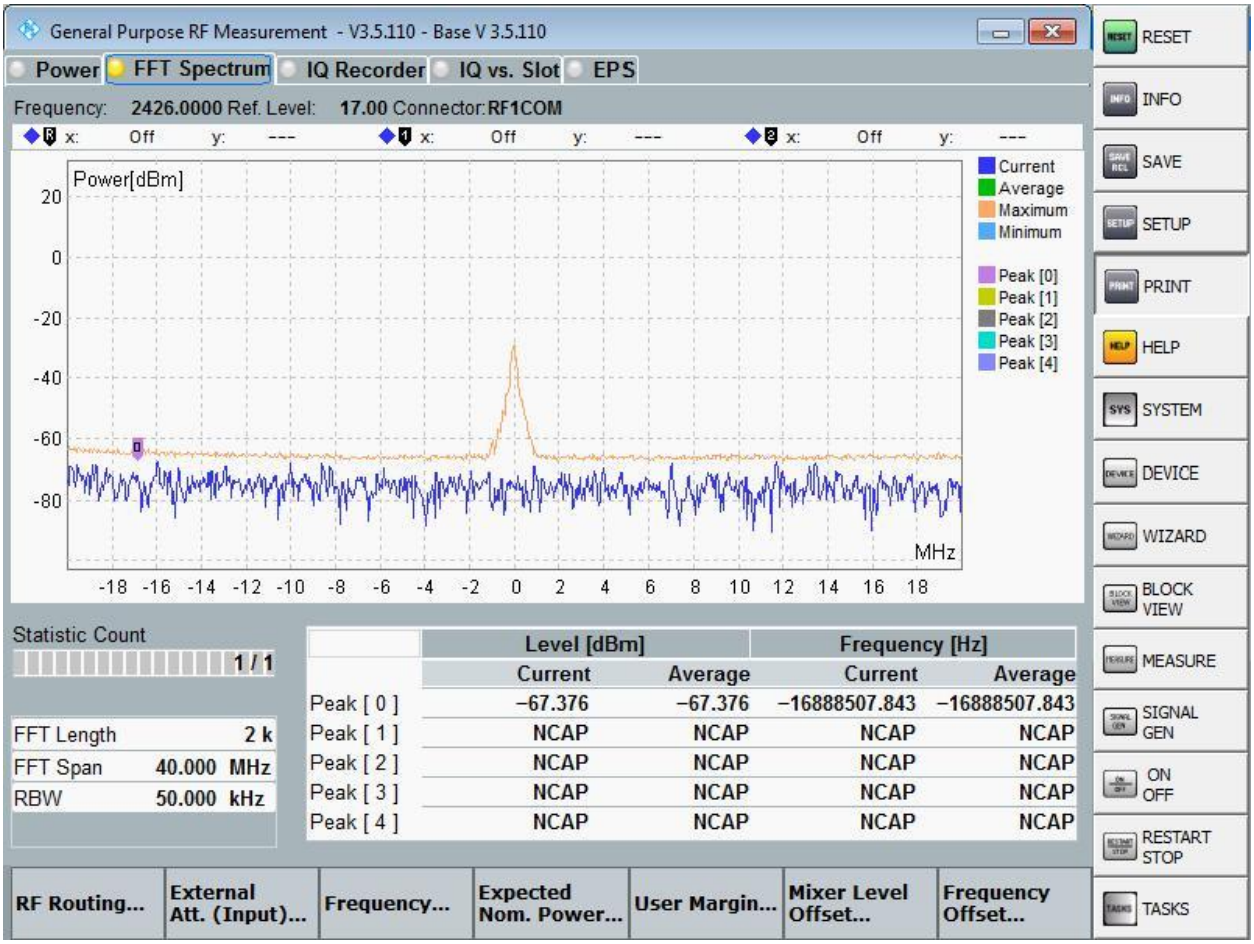
17		(1 with screen off) scans (2 with screen on, app running in the background)	Proper and sufficient recording
18		(1 with screen on and in standby mode) scans (2 with screen off)	Proper and sufficient recording
19	1 Android scans 2 iOSs	(1 running Bluezone) scans (2 running the app)	Proper and sufficient recording
20		(1 running Bluezone) scans (2 with screen off)	Proper and sufficient recording
21		(1 running Bluezone) scans (2 with screen on, app running in the background)	Proper and sufficient recording
22		(1 with screen off) scans (2 with screen off)	Proper and sufficient recording
23		(1 with screen off) scans (2 with screen on, app running in the background)	Proper and sufficient recording
24		(1 with screen on and in standby mode) scans (2 with screen off)	Proper and sufficient recording

8. Optimal power

8.1 BLE advertising mode

The physical layer of BLE is advertised on 3 channels: 37, 38, 39. Channel 38 is located between channels 1 and 6 of the WiFi, so this channel can avoid WiFi interference. In order to optimize the power, instead of using 3 advertising channels, we use Channel 38 (2426 MHz) only.

The BLE advertising signal is also not continuous but calculated in random cycles. Typically, it advertises 4-6 times within 15 seconds. Random advertising helps avoid conflicts among different devices when they overlap the advertising cycle.



8.2 Power consumption on iOS, Android

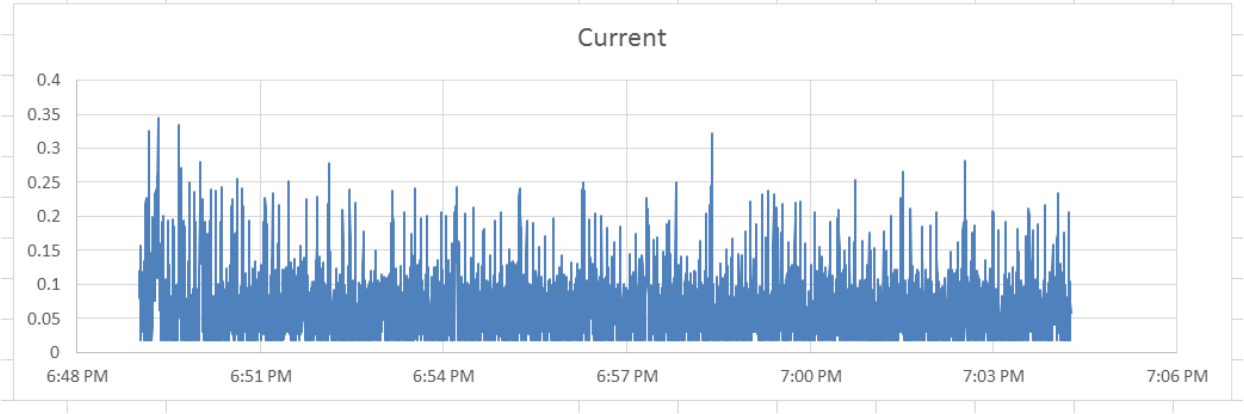
With iOS, in sleep mode, Apple will reduce Bluetooth activity of Bluezone. Therefore, the power is not a problem to be solved on the iOS platform.

However, the Android platform allows the Bluezone app to run Bluetooth in full time, even when the device is in sleep mode. To evaluate the efficiency of power usage, we measure the power consumption of Bluetooth with the device of High speed power supply.

The test measures power consumption in continuous Bluetooth advertising and scanning. The reference device operates on the Qualcomm Snapdragon 600 series platform.

In continuous advertising (BLE) and scanning (BLE, Classic) modes, the power diagram is as follows:

Estimate Battery life time			
1	Min Current consumption	17.3	mA
2	Average Current consumption	60.5	mA
3	Battery life	47.7	hours



The device consumes 60-70 mAh, which is equivalent to 2%/h (for devices with a 3000 mAh battery). Conversion will consume 40%/day; such consumption will greatly affect the user experience due to battery drain and overheating. As such, the need is to optimize power to maximize user experience.

8.3 Optimal power

To ensure optimal power consumption, we reduce the frequency of Bluetooth scanning and advertising. However, when reducing the frequency of advertising and scanning; there will be a case that this device is advertising but the receiver is idle so it cannot be scanned, thus omitting contact recording. Therefore this process is a tradeoff of advertising, scanning and idling. The problem is to optimize the idle time to minimize power consumption while still ensuring the efficiency of recording, which is to ensure that in a time period large enough for both advertising and scanning devices to operate.

To make it easier to give a set of numbers, we choose an advertising rate of 50% and specifically 15 seconds of advertising, 15 seconds of idling. Empirical evidence shows that in a period of 15 seconds BLE advertises for 4-6 times. If the receiving device scans in that period, contact recording will be guaranteed. Therefore, in order to scan the full 15s of BLE advertising, we choose the BLE scanning time larger than the advertising cycle (15 + 15 = 30s). As a backup we choose a BLE scanning time of 35 seconds. The idling time is calculated upon a 2-minute cycle of contact recording which is equivalent to 120 seconds. Therefore, the idle time of no scanning is 85 seconds.

The set of numbers is as follows:

BLE advertising in 15s, then idling for 15s. Advertising cycle will be 30s. Power will be reduced by 50% in BLE advertising mode.

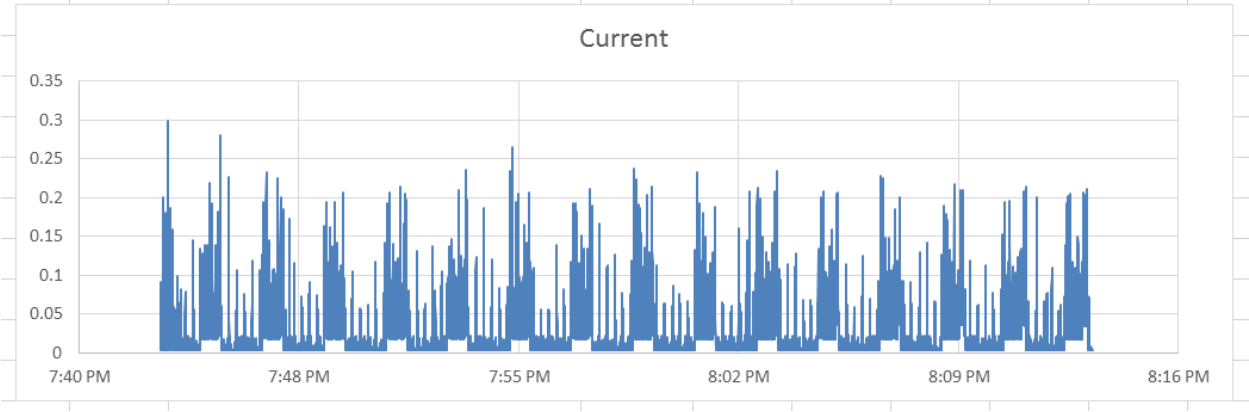
BLE scanning in 35s, then idling for 85s. Scanning cycle will be 120s. Power will be reduced by 70% in BLE scanning mode.

Bluetooth classic scanning in 35s, then idling for 85s. Classic scanning cycle will be 120s. Power will be reduced by 70% in Classic scanning mode.

This set of numbers ensures that nearby devices will recognize each other within 2 minutes, satisfying the goal of the solution.

The actual power consumption through the test with the device of High speed power supply.

Estimate Battery life time			
1	Min Current consumption	2.9	mA
2	Average Current consumption	23.6	mA
3	Battery life	122.2	hours



The power is reduced to 23-25 mAh, equivalent to consuming 1% in 1 hour and 20 minutes for devices with 3000 mAh battery.

9. Community collaboration

After consulting the technology application against COVID-19 of countries around the world, the Ministry of Information and Communications of Viet Nam (MIC) decides that the country must develop its own software to help trace and localize infections effectively. This will be the optimal solution to help life return to normal after the peak of the pandemic.

Therefore, MIC called out domestic technology companies to jointly research and find solutions. Previously, some countries had started using BLE to trace close contacts. However, these solutions have also shown several practical limitations such as: too many cases of close contacts not

recorded, battery drain, and privacy not guaranteed. The Minister of MIC himself offered the teams to record the maximum number of close contacts, overcoming the above mentioned weaknesses. Only then can the fight against the pandemic be effective.

In about 3 weeks of working on a heavy schedule, the results are encouraging when most Vietnamese teams found solutions to the above complex problems. The Authority of Information Technology Application (a unit belonging to MIC) and the teams set out 24 test cases in reality. As a result, most of these contact situations can be solved, except the 3 mentioned above. Our team believed that these issues are due to limitations from the design of the Bluetooth protocol on Android and iOS platforms. Through the communication channel of MIC, our team conducted direct discussion with Apple/Google's team that develops close contact tracingAPI, and concluded that these cases can only be resolved in the new API created thanks to the cooperation between Google and Apple.

During the working process, the Viet Nam team also proposed a direct working channel with the team of Google and Apple for researching and testing new solution. Specifically, getting early early API access to prepare for application upgrades, as well as contributing to the implementation process so that to complete these new APIs.

10. Summary

Although developing team has carefully analyzed the cases of both Android and iOS operating systems, the two themselves are not designed to serve the purpose of close contact tracing, so there are still some cases without solution. For example, two iOS devices with the screen off will not "see" each other.

Fortunately, Google and Apple have decided to work together to overcome COVID-19 pandemic. Maybe the updated API of these operating systems will help solve the above problems, making the solution more complete.

The existing solution by Google and Apple only supports those phones that are capable of upgrading to new operating systems. While, in reality, the number of phones without such capability in Vietnam is considerably large, which prevents us from switching to the API by Google and Apple.

Developing team expects the Project will be useful for technology teams of anti-pandemic agencies of other countries. Our team also wants to receive your suggestions and experiments to make this Project better, contributing to the halt of COVID-19 worldwide.